

**IN THE CLAIMS:**

1. (Original) A cipher strength evaluation apparatus for evaluating strength on ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key calculated from a user key based on a key schedule, and outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation  
5 apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information  
10 about an estimated extended key estimated as equal to the extended key and an estimated user key estimated as equal to the user key; and

an estimated unstirred text calculating part for calculating estimated unstirred text estimated as equal to unstirred text at a certain stirring step based on ciphertext or estimated stirred text estimated as equal to stirred text at that stirring step,

15 wherein the estimated unstirred text calculating part includes:

an estimated extended key calculating part for calculating an estimated extended key based on the key relationship information stored in the key relationship information storing part and the estimated key information stored in the estimated key information storing part and storing the estimated extended key in the estimated key information storing part, and

20 an estimated unstirred text calculating part main body for calculating estimated unstirred text based on ciphertext or the estimated stirred text, and the estimated extended key.

2. (Original) A cipher strength evaluation apparatus for evaluating strength on ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key calculated from a user key based on a key schedule, and outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information about an estimated extended key estimated as equal to the extended key and an estimated user key estimated as equal to the user key; and

an estimated unstirred text calculating part for calculating estimated unstirred text estimated as equal to unstirred text at a certain step based on ciphertext or estimated stirred text estimated as equal to stirred text at that step,

wherein the estimated unstirred text calculating part includes:

an estimated extended key calculating part for calculating the estimated extended key by exhaustive search based on a probabilistic relationship probabilistically held between keys contained in the key relationship information stored in the key relationship information storing part and the estimated key information stored in the estimated key information storing part and storing it in the estimated key information storing part, and

an estimated unstirred text calculating part main body for calculating estimated unstirred text based on ciphertext or the estimated stirred text, and the estimated extended key.

3. (Original) A cipher strength evaluation apparatus for evaluating strength on ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key calculated from a user key based on a key schedule, and outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information about an estimated extended key estimated as equal to the extended key and an estimated user key estimated as equal to the user key; and

an estimated unstirred text calculating part for calculating estimated unstirred text estimated as equal to unstirred text at a certain step based on ciphertext or estimated stirred text estimated as equal to stirred text at that step,

wherein the estimated unstirred text calculating part includes:

an estimated extended key calculating part for calculating an estimated extended key by an algebraic technique based on ciphertext or estimated stirred text, plaintext or estimated unstirred text, a deterministic relationship deterministically held between keys contained in the key relationship information stored in the key related information storing part, and the estimated key information stored in the estimated key information storing part, and storing the estimated extended key in the key information storing part, and

an estimated unstirred text calculating part main body for calculating estimated unstirred text estimated as equal to unstirred text based on ciphertext or the estimated stirred text, and the estimated extended key.

4. (Original) A cipher strength evaluation apparatus for evaluating strength on ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key calculated from a user key based on a key schedule, and outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information about an estimated extended key estimated as equal to the extended key and an estimated user key estimated as equal to the user key; and

an estimated unstirred text calculating part for calculating estimated unstirred text estimated as equal to unstirred text at a certain step based on ciphertext or estimated stirred text estimated as equal to stirred text at that step, and a second estimated extended key calculating part for calculating an estimated extended key at a certain step,

wherein the estimated unstirred text calculating part includes:

a first estimated extended key calculating part for calculating the estimated extended key by exhaustive search based on the estimated key information stored in the estimated key information storing part and storing it in the estimated key information storing part, and

an estimated unstirred text calculating part main body for calculating estimated unstirred text estimated as equal to unstirred text based on ciphertext or estimated stirred text, and the estimated extended key, and

25 the second estimated extended key calculating part for calculating an estimated extended key by an algebraic technique based on estimated stirred text, plaintext or estimated unstirred text, a deterministic relationship deterministically held between keys contained in the key relationship information stored in the key related information storing part, and the estimated key information stored in the estimated key information storing part, and storing the estimated extended key in the key information storing part.

5 5. (Original) A cipher strength evaluation apparatus for evaluating strength on ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key calculated from a user key based on a key schedule, and outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

10 an estimated key information storing part for storing estimated key information about an estimated extended key estimated as equal to the extended key and an estimated user key estimated as equal to the user key; and

an extended key calculating condition evaluation part for outputting cost information about a calculation resource or complexity required for calculating an estimated extended key based on the key relationship information stored in the key relationship

15 information storing part and the estimated key information stored in the estimated key  
information storing part.

6. (Original) A cipher strength evaluation apparatus for evaluating strength on  
ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred  
text, stirring with an extended key calculated from a user key based on a key schedule, and  
outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation  
5 apparatus comprising:

a key relationship information storing part for storing key relationship information  
determined by the key schedule and showing a relationship between a segment bit pattern of the  
user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information  
10 about an estimated extended key estimated as equal to the extended key and an estimated user  
key estimated as equal to the user key; and

an extended key calculating condition evaluation part for outputting cost  
information about a calculation resource or complexity required for calculating the estimated  
extended key by exhaustive search based on a probabilistic relationship probabilistically held  
15 between keys contained in the key relationship information stored in the key relationship  
information storing part and the estimated key information stored in the estimated key  
information storing part.

7. (Original) A cipher strength evaluation apparatus for evaluating strength on  
ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred  
text, stirring with an extended key calculated from a user key based on a key schedule, and

outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation

5 apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information  
10 about an estimated extended key estimated as equal to the extended key and an estimated user key estimated as equal to the user key; and

an extended key calculating condition evaluation part for outputting cost information about a calculation resource or complexity required for calculating an estimated extended key by an algebraic technique based on ciphertext or estimated stirred text, plaintext or  
15 estimated unstirred text, a deterministic relationship deterministically held between keys contained in the key relationship information stored in the key related information storing part, and the estimated key information stored in the estimated key information storing part.

8. (Original) A cipher strength evaluation apparatus for evaluating strength on ciphertext obtained by an encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key calculated from a user key based on a key schedule, and outputting stirred text for encrypting plaintext step by step, the cipher strength evaluation

5 apparatus comprising:

a key relationship information storing part for storing key relationship information determined by the key schedule and showing a relationship between a segment bit pattern of the user key and a segment bit pattern of the extended key thereof;

an estimated key information storing part for storing estimated key information  
10 about an estimated extended key estimated as equal to the extended key and an estimated user  
key estimated as equal to the user key; and

an estimated unstirred text calculating part for calculating estimated unstirred text  
estimated as equal to unstirred text at a certain step based on ciphertext or estimated stirred text  
estimated as equal to stirred text at that step, and an extended key calculating condition  
15 evaluation part for calculating cost information required for calculating an extended key,

wherein the estimated unstirred text calculating part includes:

an estimated extended key calculating part for calculating the estimated extended  
key by exhaustive search based on the estimated key information stored in the estimated key  
information storing part and storing it in the estimated key information storing part, and  
20 an estimated unstirred text calculating part main body for calculating estimated  
unstirred text estimated as equal to unstirred text based on ciphertext or estimated stirred text,  
and the estimated extended key, and

the extended key calculating condition evaluation part outputs cost information  
about a calculation resource or complexity required for calculating an estimated extended key by  
25 an algebraic technique based on estimated stirred text, plaintext or estimated unstirred text, a  
deterministic relationship deterministically held between keys contained in the key relationship  
information stored in the key related information storing part, and the estimated key information  
stored in the estimated key information storing part.

9. (Cancelled)